1783

Observationes circa divisionem quadratorum per numeros primos

Leonhard Euler

OBSERVATIONES
CIRCA
DIVISIONEM QVADRATORVM
PER NVMEROS PRIMOS.

Hypotheſis.

Si numerorum a, b, c, d, etc. quadrata a^2, b^2, c^2, d^2, etc. per numerum quempiam primum P diuidantur, reſidua in diuiſione relicta litteris cognominibus graecis α, β, γ, δ, etc. indicemus.

Corollarium 1.

§. 2. Cum ergo quadratum aa per numerum P diuiſum relinquat reſiduum α; poſito quoto $= A$ erit $aa = AP + \alpha$, ideoque $aa - \alpha$ diuiſibile erit per P; ſimilique modo hae expreſſiones: $bb - \beta$, $cc - \gamma$, $dd - \delta$, etc. diuiſibiles erunt per eundem diuiſorem P.

Corollarium 2.

§. 3. Quadrata $(\alpha + P)^2$, $(\alpha + 2P)^2$, $(\alpha + 3P)^2$, et in genere $(\alpha + \omega P)^2$ idem reſiduum α relinquent, ſi per numerum propoſitum P diuidantur. Vnde patet, numero-

merorum, diuiſore P malorum, quadrata eadem praebere reſidua, quae ex quadratis numerorum, diuiſore P minorum, naſcuntur.

Corollarium 3.

§. 4. Cum deinde quadratum $(P - a)^2$ per P diuiſum idem praebeat reſiduum, quod quadratum a^2, patet ſi fuerit $a > \frac{1}{2}P$, fore $P - a < \frac{1}{2}P$. Vnde manifeſtum eſt, omnia reſidua diuerſa ex quadratis numerorum, qui ſemiſſe diuiſoris P ſint minores, reſultare.

Corollarium 4.

§. 5. Quare ſi omnia reſidua deſiderentur, quae ex diuiſione quadratorum per datum diuiſorem P proueniunt, ſufficiet ea tantum quadrata conſideraſſe, quorum radices ſemiſſem ipſius P non ſuperent.

Corollarium 5.

§. 6. Hinc ſi diuiſor ſit $P = 2p + 1$, ſi per eum omnes numeri quadrati 1, 4, 9, 16, 25, etc. diuidantur, plura reſidua diuerſa inde prodire nequeunt, quam vnitates in numero p continentur; eaque reſultant ex quadratis numerorum $1, 2, 3, 4, \ldots\ldots p$: ſequentium enim numerorum $p + 1$, $p + 2$, $p + 3$, etc. quadrata eadem reſidua ordine retrogrado reproducunt.

Scholion.

§. 7. Manifeſtum hoc inde eſt, quod haec duo quadrata: p^2 et $(p + 1)^2$, per numerum $2p + 1$ diuiſa,

idem praebent reſiduum; ſiquidem eorum differentia per $2p+1$ eſt diuiſibilis. Generatim enim, quorumcunque numerorum differentia $M-N$ per $2p+1$, eſt diuiſibilis, neceſſe eſt vt vterque M et N, ſeorſim diuiſus, idem reſiduum relinquat. Hinc etiam cum ſit $(p+2)^2-(p-1)^2 = 3(2p+1)$, vtrumque quadratum ſeorſim, $(p+2)^2$ et $(p-1)^2$, idem reſiduum praebere debet, et in genere quadratum $(p+n+1)^2$ idem reſiduum dabit, quod quadratum $(p-n)^2$. Hoc igitur oſtenſo perſpicuum eſt plura reſidua reſultare non poſſe, quam in numero p vnitates continentur: vtrum autem haec reſidua omnia ſint diuerſa, an quaepiam inter ſe conueniant? hinc non definitur; atque adeo, ſi diuiſores quicunque admittantur, vtrumque euenire poteſt. Siñ autem diuiſor $2p+1$, fuerit numerus primus, omnia illa reſidua erunt inter ſe diuerſa quod ſequenti modo demonſtro.

Theorema I.

§. 8. Si diuiſor $P = 2p+1$ fuerit numerus primus, per eumque omnia quadrata 1, 4, 9, 16, ... vsque ad p^2 diuidantur, omnia reſidua hinc reſultantia inter ſe erunt diuerſa, eorumque adeo multitudo $= p$.

Demonſtratio.

Sint a et b duo numeri quicunque ipſo p minores, vel ſaltem non maiores; ac demonſtrandum eſt, ſi eorum quadrata a^2 et b^2 per numerum primum $2p+1$ diuidantur, reſidua certe diuerſa eſſe proditura. Si enim idem praeberent reſiduum, eorum differentia $aa-bb$ per $2p+1$, foret diuiſibilis, ideoque ob $2p+1$ numerum primum

primum et $aa-bb = (a+b)(a-b)$, alter horum factorum per $2p+1$ diuiſibilis eſſe deberet. Cum autem ſit tam $a < p$ quam $b < p$, ſaltem non $a > p$, ſumma $a+b$, multoque magis differentia $a-b$ diuiſore $2p+1$ eſt minor; indeque neutra per $2p+1$ diuiſibilis eſſe poteſt. Ex quo manifeſto ſequitur: omnia quadrata, quorum radices non ſint ipſo p maiores, per numerum primum $2p+1$ diuiſa, certe diuerſa reſidua eſſe relictura.

Corollarium 1.

§. 9. Quodſi ergo omnia quadrata 1, 4, 9, 16, etc. per numerum primum $2p+1$ diuidantur, omniaque reſidua diuerſa notentur, eorum numerus neque maior erit neque minor quam p, ſed huic numero p praeciſe aequalis.

Corollarium 2.

§. 10. Omnia vero haec reſidua diuerſa numero p, oriuntur ex totidem quadratis in ſerie naturali primum occurrentibus, ſcilicet 1, 4, 9, 16, ... pp; neque ex ſequentibus maioribus vlla noua reſidua eliciuntur.

Corollarium 3.

§. 11. Non omnes ergo numeri ipſo diuiſore $2p+1$ minores inter reſidua occurrent, ſed tantum tot eorum, quot vnitates continentur in diuiſoris minori ſemiſſe p. Quare cum numerorum, diuiſore $2p+1$ minorum, multitudo ſit $= 2p$, horum alter ſemiſſis tantum in ordine reſiduorum reperietur, alter vero inde penitus excluditur.

Scholion.

§. 12. Numeros hos diuisore primo $2p+1$ minores, qui ex ordine residuorum excluduntur, nomine *non-residuorum* indicabo, quorum ergo multitudo semper numero residuorum est aequalis. Hoc discrimen inter residua et non-residua probe perpendisse iuuabit, quare pro diuisoribus aliquot primis minoribus tam residua quam non-residua hic exhibebo.

Div. 3; $p=1$	Div. 5; $p=2$	Div. 7; $p=3$
quadr. 1	quadr. 1, 4	quadr. 1, 4, 9
residuum 1	resid. 1, 4	residuum 1, 4, 2
non-res. 2	non-res 2, 3	non-res. 3, 5, 6

Diuisor 11; $p=5$	Diuisor 13; $p=6$
Quadrata 1, 4, 9, 16, 25	Quadrata 1, 4, 9, 16, 25, 36
Residua 1, 4, 9, 5, 3	Residua 1, 4, 9, 3, 12, 10
non-resid. 2, 6, 7, 8, 10	non-resid. 2, 5, 6, 7, 8, 11

Diuisor 17; $p=8$								
Quadrata	1,	4,	9,	16,	25,	36,	49,	64.
Residua	1,	4,	9,	16,	8,	2,	15,	13
non-resid.	3,	5,	6,	7,	10,	11,	12,	14

Diuisor 19; $p=9$									
Quadrata	1,	4,	9,	16,	25,	36,	49,	64,	81
Residua	1,	4,	9,	16,	6,	17,	11,	7,	5
non-residua	2,	3,	8,	10,	12,	13,	14,	15,	18

Circa

› + 1 mi-
, nomine
do semper
1 inter re-
quare pro
dua quam

= 3
4. 9
4. 2
5. 6

6
16, 25, 36
3, 12, 10
7, 8, 11

Circa

Circa haec residua et non-residua pro quouis diuisore primo tam memorabiles proprietates obseruantur, quas eo maiori studio perpendisse operae est pretium, quod inde non contemnenda incrementa in numerorum Theoriam redundare videntur.

Theorema II.

§. 13. Si in ordine residuorum ex diuisore P ortorum occurrant numeri α et β, ibidem quoque occurret eorum productum $\alpha\beta$, siquidem minus fuerit diuisore P; sin autem sit maius eius loco capi conuenit $\alpha\beta - P$, vel $\alpha\beta - 2P$, vel generatim $\alpha\beta - nP$, donec infra P deprimatur.

Demonstratio.

Oriantur residua α et β ex diuisione quadratorum aa et bb per diuisorem P facta, ita vt sit

$$aa = AP + \alpha \text{ et } bb = BP + \beta.$$

Hinc erit

$$aabb = ABP^2 + (A\beta + B\alpha)P + \alpha\beta.$$

Quare si quadratum $aabb$ per diuisorem P diuidatur, residuum relinquetur $\alpha\beta$, vel si $\alpha\beta$ superet diuisorem P, eius loco sumi debet residuum, quod ex diuisione ipsius $\alpha\beta$ per P facta relinquetur, quod proinde erit vel $\alpha\beta - P$, vel $\alpha\beta - 2P$ vel $\alpha\beta - 3P$, vel generatim $\alpha\beta - nP$, ita vt fit $\alpha\beta - nP < P$.

Corollarium 1.

§. 14. Si ergo inter reſidua occurrat numerus α, ibidem quoque occurret $\alpha\alpha$, item α^3, α^4, etc. omnesque adeo eius poteſtates, ſiquidem a ſingulis eiusmodi multiplum diuiſoris P ſubtrahatur, vt reſiduum minus fiat diuiſore P.

Corollarium 2.

§. 15. Cum igitur exiſtente diuiſore P numero primo $2p+1$, reſiduorum numerus ſit $=p$; ſi unius cuiuspiam reſidui α omnes poteſtates α^0, α^1, α^2, α^3, α^4, etc. per eundem diuiſorem P diuidantur, inde non plura quam p reſidua diuerſa reſultare poſſunt.

Corollarium 3.

§. 16. Hinc ſequitur, poteſtatem α^k, per $P=2p+1$ diuiſam, idem praebere reſiduum quod $\alpha^0=1$, ſeu reſiduum fore vnitatem, vti alibi oſtendi, ſiquidem diuiſor $2p+1$ fuerit numerus primus.

Scholion.

§. 17. Eximiis proprietatibus, quae hinc deduci poſſunt, hic vberius euoluendis non immoror, cum hoc iam olim a me ſit factum. Ea hic tantum principia breuiter repetere conſtitui, quibus indigeo ad nouas quasdam reſiduorum affectiones explicandas, vnde inſignes nonnullas numerorum proprietates multo expeditius demonſtrare liceat. Hunc in finem animaduerto, quod quidem per ſe eſt perſpicuum, quemadmodum reſiduo $\alpha\beta$ aequiualent numeri

nerus α,
mnesque
li multi-
fiat di-

numero
inius cu-
α^4, etc.
:a quam

$=2p+1$
reſiduum
$2p+1$

deduci
:um hoc
ipia bre-
quasdam
onnullas
trare li-
i per ſe
lent nu-
meri

meri $\alpha\beta-P$, $\alpha\beta-2P$, et in genere $\alpha\beta-nP$, exiſtente P diuiſore, ita etiam omnes numeros per P diuiſos, idem reſiduum relinquentes, in hoc negotio tanquam hoc ipſum reſiduum ſpectari poſſe. Ita in ordine reſiduorum, pro quocunque diuiſore P, omnes plane numeri quadrati ipſi occurrere ſunt cenſendi, cum quilibet aa huiusmodi forma $AP+\alpha$ exhiberi queat, ideoque vero reſiduo α aequiualere ſit exiſtimandus. Hinc etiam inter reſidua numeri negatiui admitti poterunt, cum reſiduo α aequiualeat $\alpha-P$, hocque pacto omnia reſidua ad numeros ſemiſſi diuiſoris P minores reuocare licebit.

Theorema III.

§. 18. Si in ordine reſiduorum, ex diuiſore P ortorum, occurrant bina reſidua α et β, in eo quoque occurret reſiduum $\frac{\alpha+nP}{\beta}$, numero n ita aſſumto, vt $\frac{\alpha+nP}{\beta}$ fiat numerus integer, id quod ſemper fieri licet.

Demonſtratio.

Sint aa et bb ea quadrata, quae per P diuiſa relinquunt reſidua α et β, vt ſit $aa=AP+\alpha$ et $bb=BP+\beta$. Iam quaeratur c, vt ſit $c=\frac{a+mb}{b}$ numerus integer, eritque

$$cc=\frac{aa+2abm+bbmmP}{bb}=\frac{\alpha+(A+2am+bmmP)P}{\beta}=\text{num.}$$

integro. Cum nunc numerator tanquam ipſum reſiduum α, denominator vero tanquam reſiduum β ſpectari poſſit, patet, ſi cc per P diuidatur, reſiduum ad formam propoſitam reductum iri. Poſito enim breuitatis gratia $A+2am+bmmP=D$, vt ſit $cc=\frac{\alpha+DP}{\beta}$; tum vero $\frac{\alpha+nP}{\beta}=\gamma$, oſten-

oſtendi oportet, fore $cc = CP + \gamma$, vt reſiduum ex diuiſione quadrati cc per numerum P natum prodeat $= \gamma$. Cum autem ſit $\alpha = \beta\gamma - nP$ vtique fieri poterit:

$$cc = \frac{\beta\gamma + (D-n)P}{\beta + BP} = CP + \gamma,$$

quoniam inde ſequitur:

$$(D-n)P = (\beta C + \gamma B + BCP)P, \text{ ſeu}$$
$$D - n = \beta C + \gamma B + BCP$$

cuiusmodi relatio inter coefficientes ipſius P omnino neceſſaria eſt, vt numeri integri prodeant.

Aliter.

Loco reſidui α aliud aequiualens accipiatur $\alpha + nP$, vt ſit $\alpha + nP = \beta\gamma$; et cum omnia quadrata huius formae $(a + mP)^2$ idem praebeant reſiduum α, quod ex quadrato aa naſci aſſumitur, ſumatur m ita, vt fiat $a + mP = bc$, et quia quadratum $bbcc$ per P diuiſum relinquit reſiduum α, vel $\beta\gamma$, quadratum vero bb reſiduum b: neceſſe eſt vt quadratum cc relinquat reſiduum $\gamma = \frac{\alpha + nP}{\beta}$. Sit enim $bbcc = EP + \beta\gamma$ et $bb = BP + \beta$; tum vero ſi neges quadratum cc praebiturum eſſe reſiduum γ, praebeat diuerſum x, vt ſit $cc = CP + x$; erit ergo

$$bbcc = EP + \beta\gamma = (BP + \beta)(CP + x)$$
$$= \beta x + (\beta C + Bx + BCP)P.$$

Iam multiplis diuiſoris P vtrinque omiſſis, quemadmodum in aeſtimatione reſiduorum fieri ſolet, ſiquidem in minima forma deſiderentur, habebitur $\beta x = \beta\gamma$, ideoque $x = \gamma$.

Corol-

ex di-
at $= \gamma$.
:

ino ne-

$: + nP$,
ius for-
uod ex
$a + mP$
elinquit
b: ne-
$\frac{\alpha + nP}{\beta}$.
:; tum
uum γ,
go
x)

modum
minima
$= \gamma$.

Corol-

Corollarium 1.

§. 19. Cum igitur vnitas ſemper ſit reſiduum, ſi pro diuiſore P fuerit aliquod reſiduum α, tum etiam $\frac{1 \pm nP}{\alpha}$ inter reſidua occurret, quod ſi vocetur β, erit $\alpha\beta = 1 \pm nP$, ſeu inter reſidua productum $\alpha\beta$ vnitati aequialebit.

Corollarium 2.

§. 20. Pro quolibet ergo reſiduo α aliud quaſi eius reciprocum β aſſignari poteſt, vt $\alpha\beta$ vnitati aequiualeat, ſumendo ſcilicet $\beta = \frac{1 \pm nP}{\alpha}$; atque haec duo reſidua reciproca α et β inter ſe erunt diuerſa, niſi ambo fuerint vel $+1$ vel -1. Si enim ſit $\beta = \alpha$ et

$$\alpha\alpha = 1 \pm nP = 1 \pm 2mP + mmPP,$$

erit $\alpha = \pm(1 \pm mP)$ et multiplum diuiſoris mP omittendo, $\alpha = \pm 1$.

Corollarium 3.

§. 21. Dum igitur in ordine reſiduorum cuilibet reſiduo ſuum reciprocum adiungitur, hoc modo bina copulabuntur; ſemper autem vnitas ſolitaria relinquetur, tum vero etiam reſiduum -1, ſeu $P-1$, quoties quidem inter reſidua occurrit.

Scholion.

§. 22. Idea haec binorum reſiduorum reciprocorum maximi eſt momenti, et ad demonſtrationem facilem Theorematis pulcerrimi nos manuducet, quod alias per ſatis multas ambages demonſtraueram: ſcilicet quod numerus primus formae $4q + 1$ ſemper ſit ſumma duorum qua-

dratorum. Ceterum hic meminiſſe iuuabit, ſi pro quopiam diuiſore P reſidua ſint α, β, γ, δ, etc. non-reſidua vero $\mathfrak{A}$, $\mathfrak{B}$, $\mathfrak{C}$, $\mathfrak{D}$, etc. tum reſiduorum omnia producta mutua $\alpha\beta$, $\alpha\gamma$, etc. etiam inter reſidua reperiri, eorum autem producta per quodpiam non-reſiduum, veluti $\alpha\mathfrak{A}$, inter non-reſidua eſſe referenda. At producta ex binis non-reſiduis, vti $\mathfrak{A}\mathfrak{B}$, in ordinem reſiduorum tranſeunt.

Theorema IV.

§. 23. Si diuiſor P fuerit numerus primus formae $4q+3$, tum -1, ſeu $P-1$ certe in ordine non-reſiduorum reperitur.

Demonſtratio.

Cum poſito diuiſore $P=2p+1$, hic ſit $p=2q+1$, ideoque numerus impar, numerus omnium reſiduorum erit impar. At ſi -1 in ordine reſiduorum occurreret, cuilibet reſiduo α reſponderet aliud reſiduum $-\alpha$, vnde ordo reſiduorum ita ſe eſſet habiturus:

$$\begin{matrix} +1; & +\alpha; & +\beta; & +\gamma; & +\delta \\ -1; & -\alpha; & -\beta; & -\gamma; & -\delta \end{matrix} \text{ etc.}$$

foretque ergo numerus reſiduorum par. Cum igitur numerus reſiduorum certo ſit impar, fieri nequit, vt in ordine reſiduorum occurrat -1, ſeu $P-1$, conſequenter in ordine non-reſiduorum neceſſario reperiri debet.

Corollarium 1.

§. 24. Quodſi ergo pro diuiſore primo $P=4q+3$ inter reſidua occurrat numerus α, tum numerus $-\alpha$, ſeu $P-\alpha$ certe inter non-reſidua reperietur; ſimilique modo, ſi $-\beta$ fuerit reſiduum, tum $+\beta$ erit non-reſiduum.

Corollarium 2.

§. 25. Si quadratum aa per diuiſorem $P=4q+3$ diuiſum relinquat reſiduum α, quia nullum datur quadratum xx, quod praebeat reſiduum $-\alpha$, fieri omnino nequit, vt vlla ſumma duorum quadratorum $aa+xx$, per numerum illum $4q+3$ diuiſibilis, exiſtat.

Corollarium 3.

§ 26. Oriatur praeterea reſiduum β ex quadrato bb, et quia forma βaa reſiduum dat $\alpha\beta$, forma vero αbb reſiduum $\alpha\beta$, haec forma $\beta aa-\alpha bb$ per diuiſorem $P=4q+3$ erit diuiſibilis.

Corollarium 4.

§. 27. Cum autem nullum detur quadratum xx, quod reſiduum praebeat $-\beta$, nulla datur forma αxx reſiduum praebens $-\alpha\beta$, nulla huiusmodi forma $\beta aa+\alpha xx$ per numerum $P=4q+3$ erit diuiſibilis, ſiquidem α et β ſint reſidua, et α reſiduum quadrato aa reſpondens.

Corollarium 5.

§. 28. Cum autem neque haec forma $\beta aacc+\alpha ccxx$ per diuiſorem $P=4q+3$ ſit diuiſibilis, niſi quadratum cc diuiſionem admittat, qui caſus ſponte excluditur, quadrato $aacc$ quodcunque aliud reſiduum praeter α reſpondere poteſt; vnde, loco $aacc$ et $ccxx$ ſcribendo

dd et yy, nulla huiusmodi forma $\beta dd + \alpha yy$ exhiberi potest per numerum $P = 4q + 3$ diuisibilis, dum α et β sint residua.

Scholion.

§. 29. Quo haec clarius perspiciantur, percurramus quosdam numeros primos formae $4q + 3$, ac residua eius semisse maiora, subtrahendo inde $4q + 3$, negatiue repraesentemus, vt infra semissem reuocentur, indeque patebit, nullius residui α negatiuum $-\alpha$ simul in ordine residuorum occurrere:

Diuisor	residua
3	1
7	1, −3, +2
11	1, +4, −2, + 5, +3
19	1, +4, +9, − 3, +6, − 2. − 8, +7, +5
23	1, +4, +9, − 7, +2, −10, + 3, −5, −11, +8, +6
31	1, +4, +9, −15, −6, + 5, −13, +2, −12, +7, −3, −11, +14, +10, +8

Hic euidens est, inter residua omnes numeros semisse diuisoris non maiores occurrere vel signo + vel − affectos, nullum autem bis vtroque signo affectum occurrere. Hinc si singulorum horum residuorum signa mutentur, ordo non-residuorum complebitur. Hinc pro diuisore 31 sequentes formae exhiberi possunt nunquam per 31 diuisibiles: $aa + bb$; $aa - 15bb$; $aa - 6bb$; $aa + 5bb$; $aa - 13bb$; $aa + 2bb$; $aa + 7bb$; $aa - 3bb$; $aa - 12bb$; $aa + 14bb$; $aa + 10bb$. Atque in genere, si α et β sint duo quaecunque residua, nulla huiusmodi forma: $\alpha aa + \beta bb$, per numerum 31 diuisionem admittet.

Theo-

Theorema V.

§. 30. Si diuisor P fuerit numerus primus formae $4q + 1$, tum numerus -1 seu $P - 1$ certe in ordine residuorum reperitur.

Demonstratio.

Sit α residuum quodcunque, eritque etiam eius reciprocum $\frac{1}{\alpha}$ seu $\frac{1 + \alpha\alpha}{\alpha}$ residuum (19), quod, nisi sit vel $\alpha = +1$ vel $\alpha = -1$, ab α erit diuersum, ita vt exceptis his duobus casibus cuilibet residuo α respondeat suum reciprocum, quod sit α', ab α diuersum; vbi notetur ipsius α' reciprocum vicissim esse α. Quare si -1 inter residua non reperiretur, omnia residua ita repraesentari possent, binis reciprocis coniungendis:

1. α, β, γ, δ, etc.
   α', β', γ', δ', etc.

sicque cum omnia sint diuersa, numerus omnium residuorum foret impar. Cum autem diuisor sit numerus primus formae $4q + 1$, numerus omnium residuorum est $2q$, ideoque par; vnde necessario sequitur, inter residua quoque numerum -1, seu $P - 1$ occurrere, quia alioquin numerus residuorum foret impar.

Corollarium 1.

§. 31. Cum ergo pro diuisore primo $P = 4q + 1$ numerus -1 certe inter residua reperiatur, si aliud residuum quodcunque fuerit α, inter residua etiam occurret $-\alpha$.

Corollarium 2.

§. 32. Si igitur quadratum aa per diuisorem primum $4q+1$ diuisum relinquat residuum α, aliud dabitur quadratum bb, quod residuum praebebit $=\alpha$, vnde horum quadratorum summa $aa+bb$ certe erit per numerum primum $4q+1$ diuisibilis;

Corollarium 3.

§. 33. Quoniam omnia residua ex quadratis, quorum radices semisses diuisoris non superant, nascuntur, quadrato quocunque proposito aa aliud semper bb non maius quam $4qq$ exhiberi potest, vt summa $aa+bb$ prodeat diuisibilis per $4q+1$.

Corollarium 4.

§. 34. Si $1+aa$ diuisionem per $4q+1$ admittat, tum etiam $bb+aabb$, ac proinde quoque $bb+(ab-(4q+1)n)^2$ diuisionem admittet, sicque altero quadrato bb pro lubitu assumto alterum $(ab-(4q+1)n)^2$ facile reperitur.

Corollarium 5.

§. 35. Si haec duorum quadratorum summa $aa+bb$ per diuisorem $4q+1$ fuerit diuisibilis, tum etiam $aaxx+bbxx$, ac proinde quoque haec forma:

$$(ax-(4q+1)m)^2+(bx-(4q+1)n)^2$$

diuisionem admittet. Semper autem x ita assumere licet, vt alterius radix $ax-(4q+1)m$ dato numero c aequetur, sumendo $x=\frac{c+(4q+1)m}{a}$, quod semper in integris fieri potest.

Scho-

Scholion 1.

§. 36. Pro quouis diuisore primo, siue sit formae $4q+1$, siue $4q+3$, numerorum reciprocorum consideratio omnem attentionem meretur, cum inde tam facile hanc insignem veritatem elicuerimus, quod, proposito numero primo quocunque formae $4q+1$, semper summas binorum quadratorum exhiberi queant per illum diuisibiles. Cum igitur demonstrari praeterea possit, summam duorum quadratorum alios non admittere diuisores, nisi qui ipsi sint summae duorum quadratorum, hoc modo Theorematis Fermatiani, quod omnes numeri primi formae $4q+1$ sint duorum quadratorum aggregata, demonstratio multo expeditius absoluitur, quam quidem olim a me est factum. Quemadmodum autem numeri reciproci pro quouis diuisore P se habeant, dum cuiusuis numeri a reciprocus est $\frac{1+nP}{a}$, ex subiunctis exemplis clarius intelligetur:

Diuisor

Diuisor	Reciprocorum paria
3	- - -
5	2
	3
7	2, 3
	4, 5
11	2, 3, 5, 7
	6, 4, 9, 8
13	2, 3, 4, 5, 6
	7, 9, 10, 8, 11
17	2, 3, 4, 5, 8, 10, 11
	9, 6, 13, 7, 15, 12, 14
19	2, 3, 4, 6, 7, 8, 9, 14
	10, 13, 5, 16, 11, 12, 17, 15
23	2, 3, 4, 5, 7, 9, 11, 13, 15, 17
	12, 8, 6, 14, 10, 18, 21, 16, 20, 19
29	2, 3, 4, 5, 7, 8, 9, 12, 14, 16, 18, 19, 23
	15, 10, 22, 6, 25, 11, 13, 17, 27, 20, 21, 26, 24

Singula haec paria reciproca ita inter se sunt connexa, vt quilibet numerus vnicum tantum recipiat reciprocum, diuisore scilicet minorem, prorsus vti in Theoremate assumsimus.

§. 37.

8, 19, 23
1, 26, 24

sunt connexa,
t reciprocum,
heoremate as-

§. 37.

Scholion 2.

§. 37. Quodsi ergo diuisor primus fuerit formae $4q+1$, videamus quomodo residua secundum hanc legem reciprocorum dispositа se sint habitura:

Diuisor	Residua
5	1, 4
	1, (−1)
13	1, 4, 9, 3, 12, 10
	1, 4, 9, 12 10, 3, (−1)
17	1, 4, 9, 16, 8, 2, 15, 13
	1, 4, 9, 8, 16 13, 2, 15, (−1)
29	1, 4, 9, 16, 25, 7, 20, 6, 23, 13, 5, 28, 24, 22
	1, 4, 9, 16, 25, 6, 23, 28 22, 13 20, 7, 5, 24, (−1)
37	1, 4, 9, 16, 25, 36, 12, 27, 7, 26, 10, 33, 21, 11, 3, 34, 30, 28
	1, 4, 9, 16, 25, 12, 27, 26, 21, 36 28, 33, 7, 3, 34, 11, 10, 30, (−1)

Ex his exemplis perspicuum est, cum vnitas sit solitaria, et reliquorum residuorum quodque suum reciprocum habeat adiunctum, numerum residuorum futurum esse imparem, nisi praeter vnitatem aliud residuum solitarium accederet, quod sibi ipsi esset reciprocum. Quoniam igitur his casibus, quibus diuisor est numerus primus formae $4q+1$,

numerus reſiduorum certo eſt par $= 2q$, neceſſe eſt vt praeter vnitatem, reſiduum $4q$ vel -1 occurrat, cuius quippe reciprocum ipſi eſt aequale. Vnde veritas inſignis iſtius Theorematis, cuius demonſtratio alioquin maxime erat difficilis, admodum fit perſpicua: quod ſcilicet, quoties diuiſor ſit numerus primus formae $4q+1$, inter reſidua ſemper occurrat numerus $4q$ vel -1.

Scholion 3.

§. 38. Quemadmodum hinc patet numerum -1 inter reſidua reperiri, quoties diuiſor fuerit numerus primus formae $4q+1$, ita pro quouis alio numero primo s, diuiſorum primorum forma aſſignari, at nondum demonſtrari poteſt, vt iſte numerus s in reſiduis reperiatur. Cuiusmodi eſt hoc Theorema:

Si diuiſor primus fuerit formae $4ns+(2x+1)^2$, *exiſtente* s *numero primo, tum in reſiduis occurrent numeri* $+s$ *et* $-s$.

alterumque huic ſimile:

Si diviſor primus fuerit formae $4ns-(2x+1)^2$ *exiſtente* s *numero primo, tum in reſiduis occurret numerus* $+s$; *at* $-s$ *erit in non-reſiduis*

Quando autem viciſſim $-s$ occurrat in reſiduis, at $+s$ in non-reſiduis, ita in genere definiri nequit. Pro caſibus autem particularibus res ita ſe habere deprehenditur,

vt ſit	diuiſor primus debet eſſe
-2 reſiduum, $+2$ non-reſiduum	$P=8n+3$

ceſſe eſt vt
rrat, cuius
itas inſignis
in maxime
cet, quoties
ater reſidua

nerum -1
merus pri-
o primo s,
m demon-
riatur. Cu-

$+1)^2$, *exis-*
occurrent

$+1)^2$ *exis-*
ccurret nu-

, at $+s$
Pro caſibus
ditur,

— 3

-3 reſiduum, $+3$ non-reſiduum	$P=12n+7$
-5 reſiduum, $+5$ non-reſiduum	$P=20n+3,7$
-7 reſiduum, $+7$ non-reſiduum	$P=28n+11,15,23$
-11 reſiduum, $+11$ non-reſiduum	$P=44n+3,15,23,27,31$
-13 reſiduum, $+13$ non-reſiduum	$P=52n+7,11,19,15,31,47$
-17 reſiduum, $+17$ non-reſiduum	$P=68n+3,7,11,23,27,31,39,63$
-19 reſiduum, $+19$ non-reſiduum	$P=76n+7,11,19,23,35,39,43,47,55,63$
-23 reſiduum, $+23$ non-reſiduum	$P=92n+3,23,27,31,35,39,47,55,59,71,75,87$

Quorum caſuum contemplatio hoc ſuppeditat Theorema:

Si diuiſor primus fuerit formae $4ns-4z-1$, *excludendo omnes valores in forma* $4ns-(2x+1)^2$ *contentos, exiſtente* s *numero primo, tum in reſiduis occurret* $-s$, *at* $+s$ *erit non-reſiduum.*

Quibus Theorematibus inſuper hoc adiungi poteſt.

Si diuiſor primus fuerit formae $4ns+4z+1$, *excludendo omnes valores in forma* $4ns+(2x+1)^2$ *contentos, exiſtente* s *numero primo, tum tam* $+s$ *quam* $-s$ *in non-reſiduis occurret.*

Theoremata haec ideo ſubiungo, vt qui huiusmodi ſpecula-

lationibus delectantur, in eorum demonstrationem inquirant, cum nullum sit dubium, quin inde Theoria numerorum insignia incrementa sit adeptura.

Conclusio.

§. 39. Quatuor haec Theoremata postrema, quorum demonstratio adhuc desideratur, sequenti modo concinnius exhiberi possunt:

Existente s *numero quocunque primo, dividantur tantum quadrata imparia* 1, 9, 25, 49, *etc. per divisorem* 4s, *notenturque residua, quae omnia erunt formae* $4q+1$, *quorum quodvis littera* α *indicetur, reliquorum autem numerorum, formae* $4q+1$, *qui inter residua non occurrunt, quilibet littera* $\mathfrak{A}$ *indicetur, quo facto si fuerit*

divisor numerus primus formae	tum est
$4ns+\alpha$	$+s$ residuum et $-s$ residuum
$4ns-\alpha$	$+s$ residuum et $-s$ non-residuum
$4ns+\mathfrak{A}$	$+s$ non-residuum et $-s$ non-residuum
$4ns-\mathfrak{A}$	$+s$ non-residuum et $-s$ residuum.

OBSER-

onem inqui-
heoria nume-

ftrema, quo-
i modo con-

ntur tantum
per divisorem
erunt formae
licetur, reli-
+ 1, qui in-
ra $\mathfrak{A}$ indice-

n
fiduum
on-residuum
fiduum.

OBSER-

OBSERVATIONES ANALYTICAE.

§. 1.

Inter alia, quae passim de fractionibus continuis sum commentatus, notatu digna videtur haec forma:

$$\cfrac{1+n}{2+\cfrac{n+1}{3+\cfrac{n+2}{4+\cfrac{n+3}{5+\cfrac{n+4}{6+\text{etc.}}}}}}$$

cuius valor, quoties n est numerus integer, sequenti modo exhiberi potest, denotante e numerum, cuius logarithmus est unitas, ut sit $e = 2{,}71828182845904\ldots$

$$\cfrac{1+1}{2+\cfrac{2}{3+\cfrac{3}{4+\cfrac{4}{5+\text{etc.}}}}} = \frac{1}{e-2};$$

$$\cfrac{1+2}{2+\cfrac{3}{3+\cfrac{4}{4+\cfrac{5}{5+\text{etc.}}}}} = e-1;$$

1+